

Lab 4

Undersökning av verktyget DFF

Kopiera upp maskin Lab 3.

Kopiera in filerna från foldern Fix på lärarens hårddisk till din folder Lab 3. Bör ta 30 sekunder.

Starta Windows-maskinen, gör live-utvinning, kontaminera och stäng ner med start-knappen.

Starta Linux-maskinen.

Montera toolboxen:

```
mkdi r /mnt/tool box  
mount /dev/sda2 /mnt/tool box/  
ls /mnt/tool box
```

Gör en diskavbild. Windowsdisken är /dev/sdb1.

Starta DFF.

Undersök:

- Kan man föra in en diskavbild i DFF och navigera i filstrukturen?
- Kan man göra sökningar?
- Kan man skapa en tidslinje för filerna?
- Kan man utföra signaturanalys?
- Kan man utföra carving?
- Kan man jobba med hashsummer?
- Kan man lägga till noteringar (bookmarks)?

Skriv ett kort utlåtande om verktyget.